**Mini Project Report**

**on**

# ELECTRONIC HEALTH RECORDS WITH BLOCKCHAIN AND ACCESS CONTROL


Submitted by

**BADIGINCHALA CHANDANA PRIYA-(20BCS026)**

**ERIGI VAISHNAVI-(20BCS044)**

**LALAM DIVYA SRI-(20BCS076)**

**RAVULA VEEKSHITH REDDY-(20BCS111)**

Under the guidance of

**Dr. Pavan Kumar C Ph.D (VIT Vellore)**

**Head of department CSE**




**COMPUTER SCIENCE AND ENGINEERING**

**INDIAN INSTITUTE OF INFORMATION TECHNOLOGY DHARWAD**


03/05/2023

# Contents

# List of Figures

# 1 Introduction

For a very long time, blockchain technology has been a fascinating research topic, and numerous entities have taken use of its benefits. Blockchain is a distributed digital ledger technology that makes it possible to keep track of transactions across a network of computers in a secure and transparent manner. Due to lack of security, privacy, confidentiality and decentralization in health sectors they have taken interest in blockchain. Many of the present problems in the healthcare sector, including interoperability, data privacy and security, may be resolved through implementing blockchain for EHRs. In this paper we are going to discuss how blockchain helps in transforming electronic health records and we are going to see different types of policies for encryption and access control. A framework has been presented on how to implement blockchain technology for EHR's. In this paper we are going to discuss the scalability problem faced by blockchain technology.

## 1.1 Problem Statement

**"To develop an electronic health record system that utilizes blockchain technology and access control measures to securely manage patient data, while ensuring that only authorized individuals can access sensitive information to maintain patient privacy and confidentiality.".**

## 1.2 Architecture

The Architecture of an EHR system that includes blockchain technology and access control is crucial. Centralized solutions are not practical due to the distribution of patients' health data among various entities. EHR system architectures are divided into two types: distributed and cloud. Trust management mechanisms such as Hierarchical Identity-Based Public Key Infrastructure (HIB-PKI) and credential-based access control are commonly used in distributed systems. Cloud architectures can be public, private, hybrid, or community and can use trusted, semi-trusted, or untrusted servers. Incorporating blockchain technology enhances the security and privacy of patient data. Access control is regulated through role-based access control (RBAC) which grants access based on the user's role within the organization. For instance, a physician may access all patient data.

## 2 Related Work

[1] article is about the problems with electronic health services, which are used by patients and healthcare professionals, and how to address those problems. The authors looked at different ways to make these services more secure and private, like using encryption and access controls. They organized their findings into categories like architecture, access control, and anonymity, and discussed open research problems in each category. The article provides a helpful framework for future research in this area. The [2] article reviews different methods proposed by researchers to protect patient privacy and secure the sharing of electronic health information, and discusses their strengths and limitations. Bhatt et al.proposed a safe and quick way for patients to identify themselves during telemedicine services by using biometric authentication and one-time passwords. Wazid et al. propose a way to securely share electronic health records (EHRs) using attribute-based encryption (ABE) and blockchain technology. Atallah et al. propose a way to protect patient privacy in mobile health (mHealth) services by using a secure multi-party computation technique to aggregate data while preserving privacy. Li et al. propose a way to securely share EHRs using a proxy re-encryption (PRE) technique and attribute-based access control (ABAC).

The [3] article focuses on securing healthcare data in the cloud by proposing different techniques to enhance data privacy and security while ensuring access control. Qingqing Wu and Xiaohui Liang propose a secure data sharing and access control scheme for cloud-based healthcare services that uses attribute-based encryption.Taehoon Ko, Shams Zawoad, and Ragib Hasan suggest a privacy-preserving framework for electronic health records, which combines attribute-based encryption and differential privacy. Weijia Jia, Chunxiao Li, and Jianfeng Ma propose a cloud-assisted access control scheme for e-health systems that utilizes attribute-based encryption and blockchain technology. Dandan Zhao, Qianqian Zhang, and Shangping Ren propose a privacy-preserving data sharing scheme for mobile health services, which combines attribute-based encryption and secure multi-party computation.

# 3 Methodology

This section includes requirements and also emphasizes the procedures and components used in the proposed framework of work. It describes the advantages of the software system utilized to construct this framework. Ethereum and IPFS, which are prominent and crucial for the implementation of this architecture, are also covered in the part that follows.

**Requirements**

- Ensure the privacy and security of patient data in the EHR system.
- Implement access control mechanisms to ensure that only authorized individuals can access the records.
- Enable information exchange with other systems to ensure the accuracy of records.
- Provide scalability to adapt to changes in the number of users or amount of data.
- Design the EHR system to work effectively and efficiently to provide quick access to records.

## 3.1 Fundamental Framework

### 3.1.1 Ethereum

Ethereum is a platform that allows developers to create decentralized applications (dApps) and smart contracts. It is based on the blockchain technology which is similar to Bitcoin. The main feature of Ethereum is the creation of a platform for smart contracts. Its architecture is decentralized and peer-to-peer, and uses a consensus algorithm called Proof of Work (PoW) to verify and add transactions to the blockchain. Ethereum is currently in the process of transitioning to a Proof of Stake (PoS) consensus algorithm, which is expected to consume less energy and be more scalable. Solidity, a programming language, is also available to developers for building their own blockchains.

The Ethereum network's native cryptocurrency, Ether (ETH), which is used to pay for transaction costs and other services, is a key component of this platform. Like Bitcoin and other cryptocurrencies, Ether is used as a store of money and a medium of exchange.The

method through which external parties communicate with Ethereum is through transactions. An Ethereum transaction enables external users to alter the state of a file or data collection on the Ethereum blockchain network. It comprises the sender-author and recipient, each identified by a 20-byte address. To execute a transaction, the author needs to pay a fee, which includes the amount transferred and gas cost. Gas is the fee charged for processing a transaction on the network, and its value depends on the amount the author is willing to pay. The gas fee is subject to limits and costs that vary for each transaction.

### 3.1.2 Smart Contracts

A smart contract refers to a digital program that operates automatically based on predefined regulations and conditions of a contract. Its purpose is to streamline the negotiation and execution of an agreement among multiple parties, without the need for intermediaries. By utilizing blockchain technology, smart contracts can store and validate transactions in a secure and transparent manner.

Whenever a user sends a transaction, the smart contract is triggered to perform its functions. These contracts function directly on the blockchain, making them resistant to any attempts of tampering or manipulation. Any type of blockchain activity can be programmed using smart contracts, which use the Solidity programming language. Once the required functions have been programmed, the programmers can compile them. Then it can be compiled, executed, and deployed on the Ethereum blockchain. The smart contract code is written using JavaScript, which implements Ethereum's Solidity language.

### 3.1.3 Ethereum Virtual Machine

One of Ethereum's key benefits is its blockchain programmability, which enables users to create customized applications that utilize Ethereum. These applications, known as Distributed Applications (DApps), consist of various protocols packaged together to form a DApp platform. DApps utilize smart contracts, which execute a specific task of the application, and are authorized by the user. The Ethereum Virtual Machine (EVM) is utilized to run and deploy the code, which means that smart contract-based applications operate on the EVM.

## 3.2 Software Requirements

### 3.2.1 Web3

Web3, also called the decentralized web or blockchain web, relies on blockchain systems like Ethereum, which offer a framework for developing decentralized applications and smart contracts. By leveraging a decentralized network of computers that cooperate to verify and process transactions, Web3 applications aim to deliver enhanced security, transparency, and dependability when compared to traditional web applications. This is achieved by removing intermediaries and promoting trust and consensus among participants, which is facilitated by the decentralized nature of the blockchain network.

Web3 technology enables connection to the Ethereum network through an Ethereum node via the HTTP connection, utilizing the Hypertext Transfer Protocol.. This might be a node for local system ETH wallets.

MetaMask is a web browser extension that permits users to access their Ethereum accounts and use the platform on websites. It functions as an Ethereum wallet that is connected to a Web3 provider class, allowing users to access publicly available Ethereum nodes through a Web3 provider data structure. Users can manage their public and private keys related to their account by using MetaMask. The implementation of Ethereum, MetaMask, and web3.js, together with a web interface, establishes communication between the front-end and back-end of the system.

### 3.2.2 Truffle

The development environment for Ethereum Virtual Machine is robust, utilizing blockchains, an asset pipeline, and a test framework. Its features include binary dependency management, as well as the ability to compute, implement, and maintain smart contracts. Additionally, it has a scriptable deployment and migration framework and a fully automated environment for testing smart contracts. Direct connection with the contract as well as a pipeline with close integration can be created. To run programs, the truffle environment is used.

### 3.2.3 Ganache

Ganache is a personal blockchain platform that provides a local environment for developing and testing Ethereum-based applications. Although the Ethereum development team now maintains

it, Truffle, a well-known Ethereum development framework, originally created it. Developers may quickly create a local Ethereum network with accounts, transactions, and a simulated blockchain using Ganache. This eliminates the requirement for a public blockchain network, making it simple to test and debug smart contracts and decentralized apps (dApps)..

## 3.3 Protocol Layout

The system's layout is illustrated in Figure 1, which is accessed by patients who wish to view their medical records through the healthcare system's decentralized website or Metamask. Using Ganache we get a unique ID with gas in it. ( Gas is the fee paid by users of the network to compensate for the resources used by the network to execute a particular transaction or contract). After receiving the unique ID from Ganache a private key is generated. Using this private Key we access the Ethereum Wallet. ( Ethereum allows users to manage their Ethereum accounts, store and send Ether and other tokens, and interact with decentralized applications (dApps) built on the Ethereum blockchain).The user can log in automatically by accessing the private key from their Ethereum wallet. This type of wallet is known as a cold storage wallet, and its security level is higher than that of hot wallets. Therefore, the risk of being hacked is significantly lower. Moreover, if a patient loses their device, there will be no detrimental impact on their medical records. The Ethereum wallet can also be used for document signing and information verification. Using this wallet, it is possible to create distributed property identification systems and access control systems based on user roles for records. It can also enable multiparty patient verification. Additionally, an authorization system that involves multiple parties can be developed for medical emergencies, enabling access to the patient's medical records.

## 3.4 Use-case illustration of the system

The use-case diagram is shown in Figure 2 .The application comprises three key users: an administrator, a doctor, and a patient. The process involves entering profile data and granting access to all three parties.The administrator has full control over most of the functions and can monitor all data. The doctor is the only user who can modify block data by adding the patient's records. The patient can only be having access to add primary details of themself,

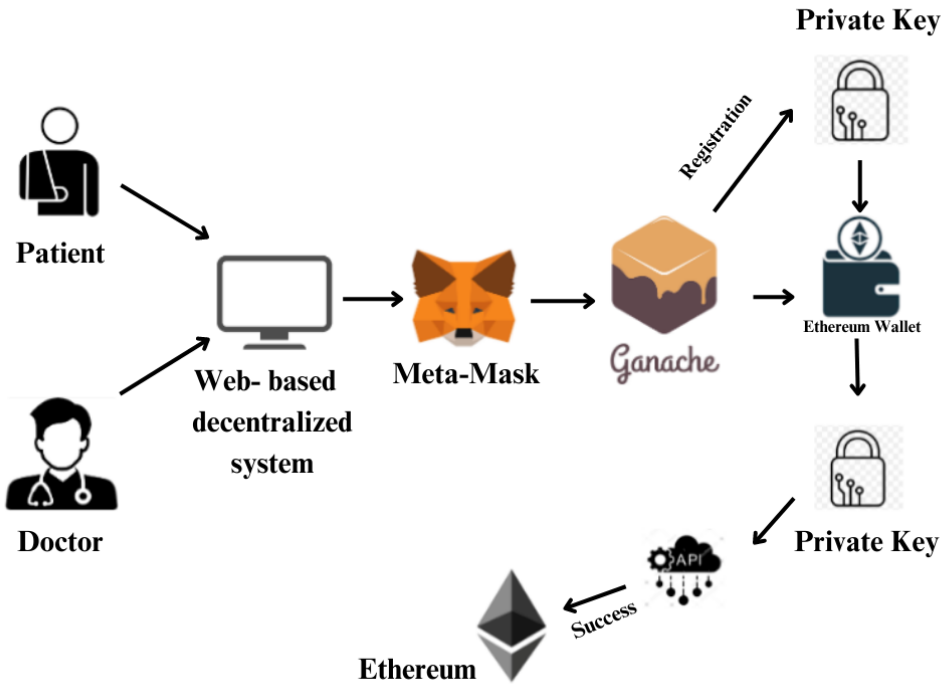


Figure 1. Protocol layout

then the authorized doctor makes updates to their records.

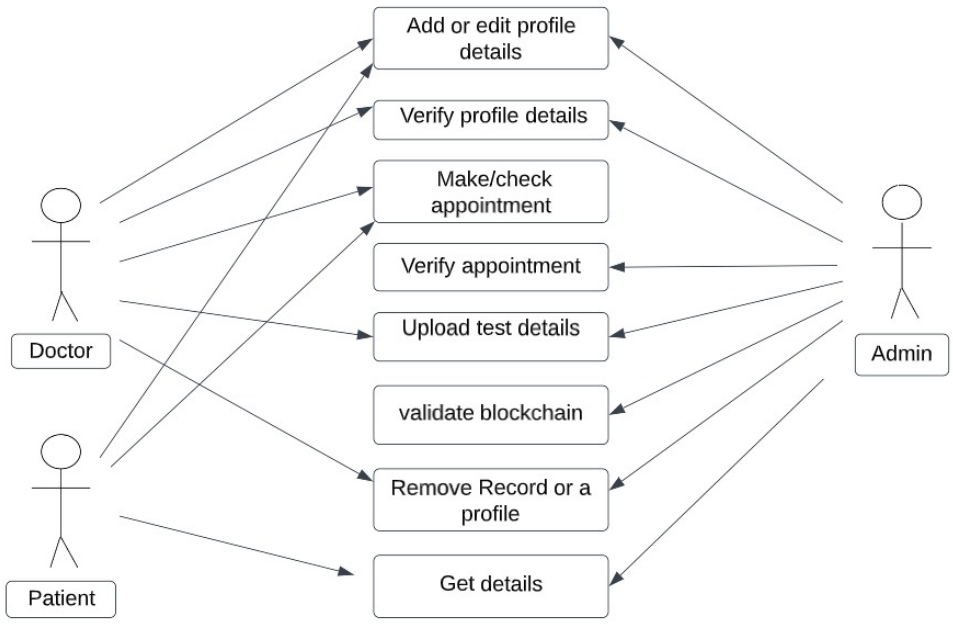


Figure 2. Use-Case diagram

### 3.4.1 ADMIN DASHBOARD

Figure 3 describes The workflow of the admin dashboard for a blockchain-based EHR system starts with a user obtaining a transaction ID with a private key that provides access to the system, including an admin feature. The transaction ID is used as the user's account to access the Ganache Ethereum (ETH) wallet, and once confirmed by the Ethereum wallet, the verified account is granted access to the admin dashboard. The admin dashboard is responsible for managing the system and may include functionalities such as verifying updates in the records, monitoring and creating doctor appointments, and managing appointments. It's worth noting that while Ganache is suitable for testing and development purposes, it's not recommended for production use cases.

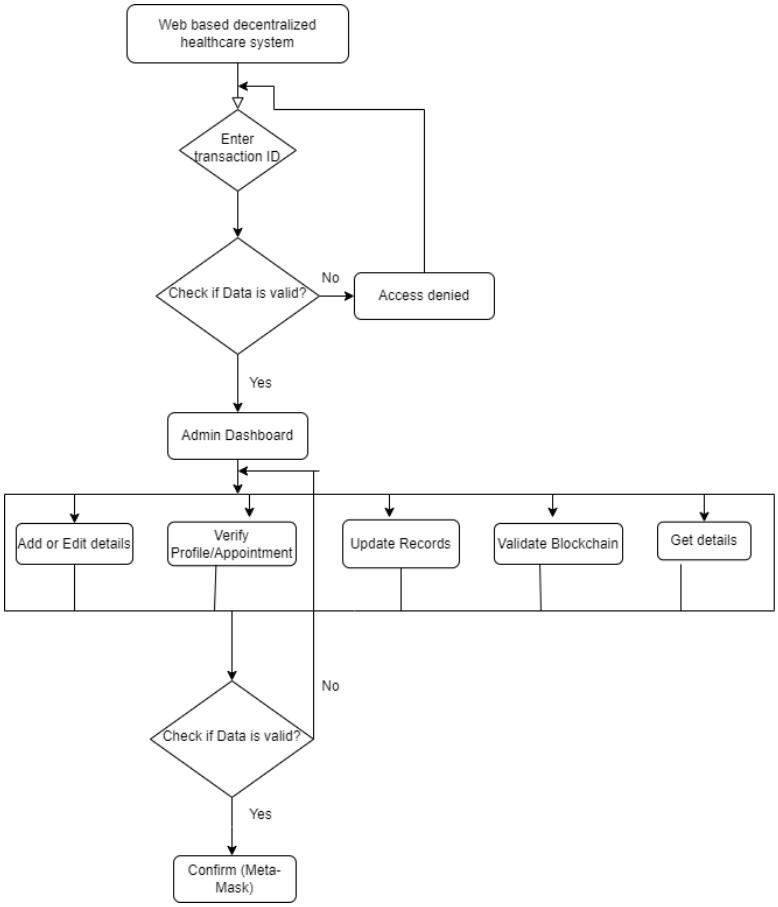


Figure 3. Admin dasboard

### 3.4.2 DOCTOR DASHBOARD

The mechanics of the doctor's dashboard are shown in Figure 4. A doctor can complete the registration with the necessary data and a transaction ID. Only the doctor will have access to the dashboard; everyone else access will be denied. The admin is also responsible for viewing appointments, but the doctor also uses the dashboard to do five other tasks. The admin dashboard of the blockchain-based EHR system allows doctors to view their personal information and update their profile details, such as their educational background. Doctors also have access to patients' personal and medical history and can add new information to the patient's dashboard as needed for upcoming therapy. Similar to administrators, doctors have the authority to modify a patient's record and delete any record from the patient's dashboard, including those that are several years old, to avoid any confusion. Furthermore, doctors are aware of the significance of having accurate and up-to-date information and may prioritize more recent data as being more precise.

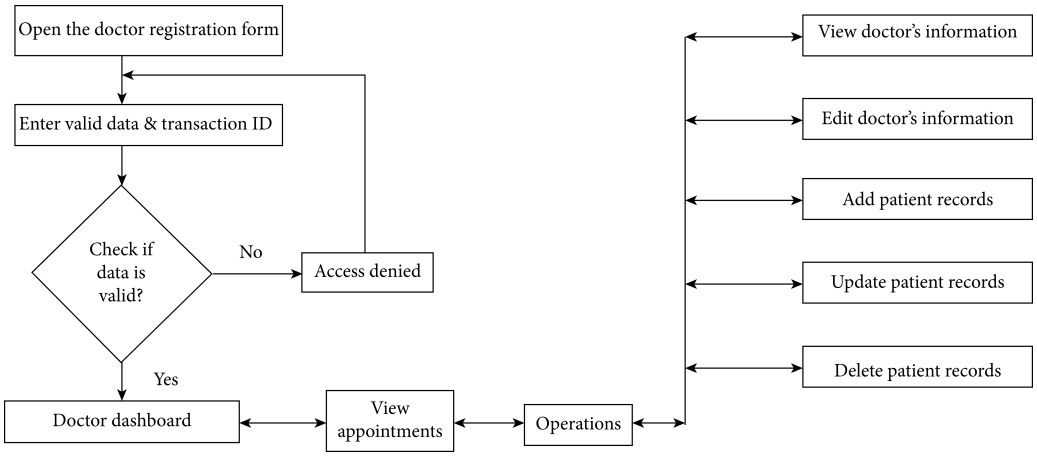


Figure 4. Doctor Dashboard

### 3.4.3 PATIENT DASHBOARD

Figure 5 illustrates how to build a patient dashboard. A patient can complete registration with the right data and a transaction ID. Only patients with registered IDs and accurate information are permitted to view the dashboard. If not, access will be denied and the patient will be prompted to provide the correct password. The patient uses the dashboard to do three tasks in

addition to monitoring appointments. Viewing extensive information and medical records are two of them. Patients cannot read their personal information until they have successfully registered. Additionally, patients have access to their doctor-supplied medical records. Patients are granted the ability to modify their personal information on the dashboard of the blockchain-based EHR system, which encompasses various details such as their name, age, phone number, and present medical condition.

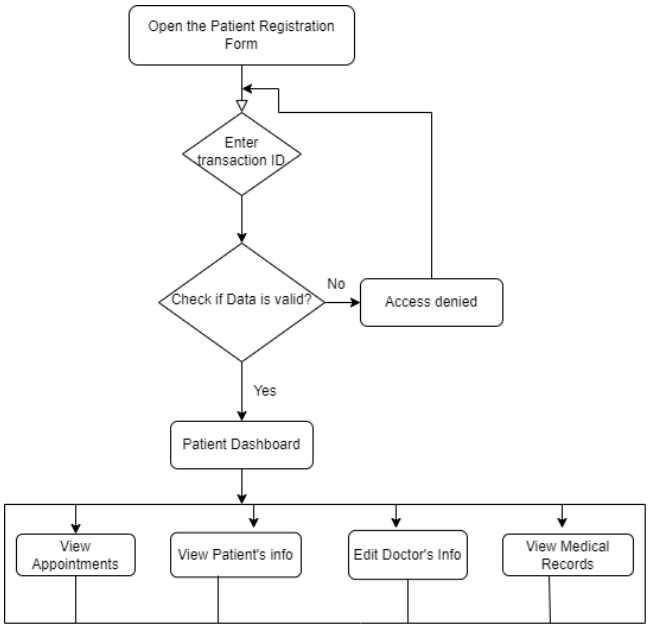


Figure 5. Patient Dashboard

# 4 Results and Discussions

By incorporating blockchain technology, the security of electronic health records was strengthened through various measures, such as cryptographic hashing of patient data and secure storage on a decentralized ledger. Moreover, the access control system was equipped with extra security measures, including two-factor authentication and role-based access controls. In our project, as mentioned in the above section with the use case and functionalities of users the following are the results From the figure 6, it represents the outcome of the admin

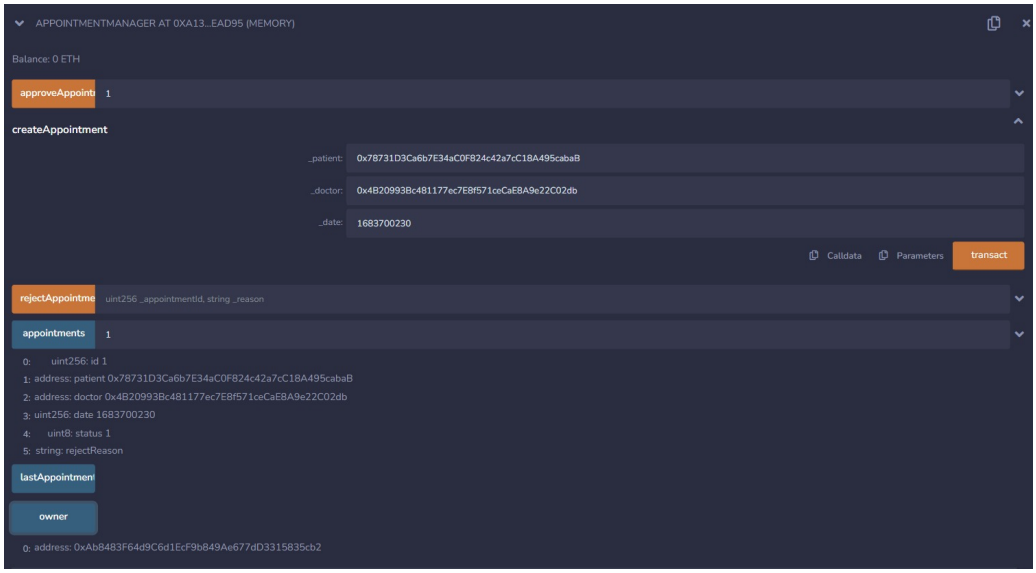


Figure 6. Outcome of Admin Contract

contract written in the solidity, the admin acts as an Appointment manager, with the address 0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2, and he/she has the control to create and alter the appointment status. Figure 7, represents the basic functions of EHR smart contract that we have used, it shows how the doctor can make a transaction and enter into the network, after that they can be authorized and have control to create the medical related records for the existing patients in the network. Figure 8, representing the outcome for functions, to get the doctor profile details and patients medical records. Suppose we have created one more record for the patient and have updated the record using the index variable( index starting with 0), we have the functions to monitor those actions, figure 9 represents the results of the above actions. Electronic health records (EHRs) have improved patient care, but challenges

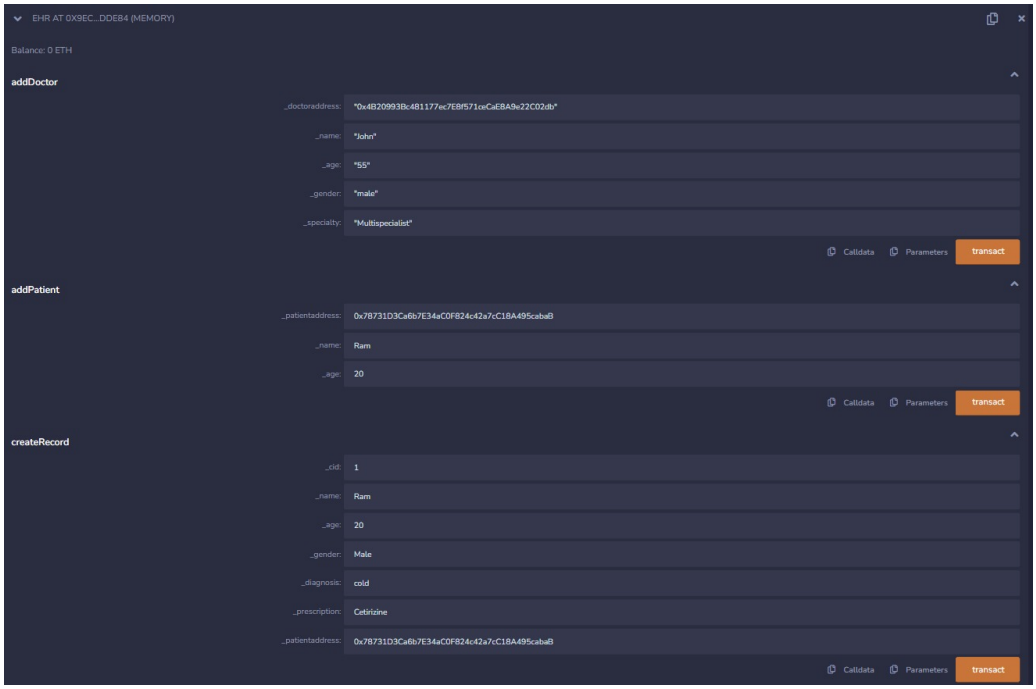


Figure 7. Functions of EHR contract

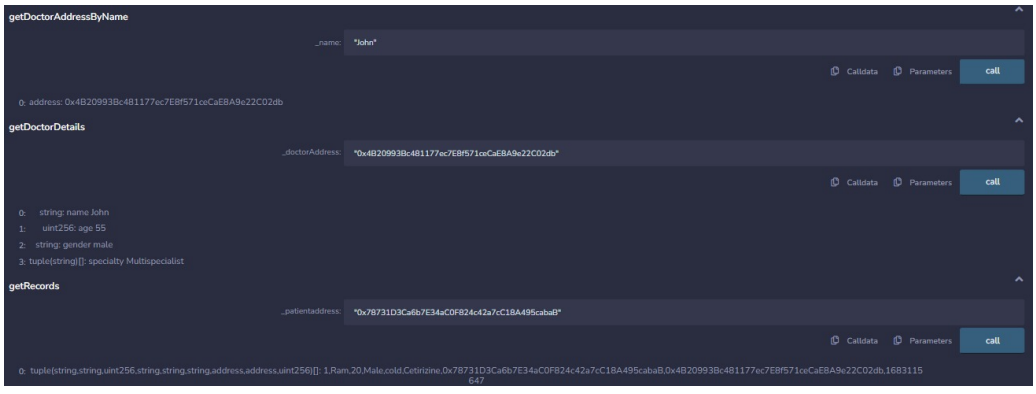


Figure 8. Outcome of Functions

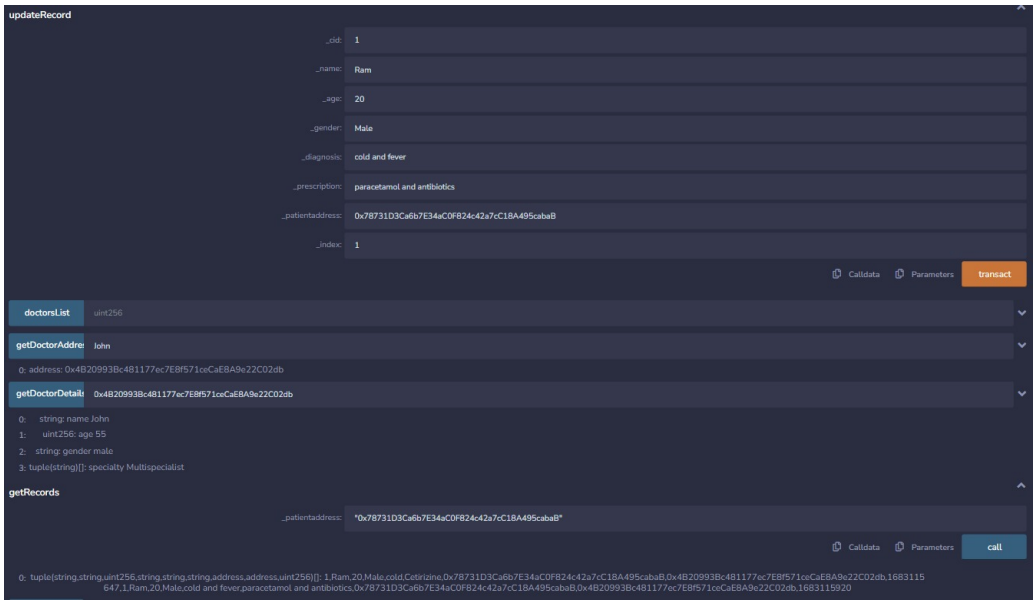


Figure 9. Results

remain in healthcare, such as care coordination, data security, and interoperability. Blockchain technology offers a potential solution to these challenges, providing a secure and decentralized platform for storing and sharing health data. By using smart contracts, patients can easily manage access to their data, improving access control and security of EHRs. This has the potential to enhance patient care and data security, while also reducing costs and facilitating research collaborations among healthcare providers and researchers. The utilization of blockchain technology in healthcare, specifically in the management of EHRs, has the capacity to enhance patient care and data security, as well as minimize expenses. Additionally, blockchain can assist in managing patient data by creating a complete and precise record of a patient's medical history. Moreover, blockchain can encourage research collaborations among healthcare providers and researchers while ensuring the patient data privacy and security.

# 5 Conclusion

The traditional way of keeping medical records is not very good because it requires a lot of space to store information for every patient and the data is hard to understand. Blockchain technology can help fix these problems because it keeps information secure and makes it easier to share. This is especially important for sensitive health data. Using Ethereum and smart contracts can also automate the process of allowing or denying access to medical records, making it quicker and easier for patients to control who can see their information. Access control is regulated through the mechanism attribute-based access control (ABAC), which ensures that only authorized individuals have access to patient data. But still there are challenges that need to be addressed, such as scalability, interoperability, and data standardization. Therefore, further research and development are needed to overcome these challenges and fully realize the potential benefits of blockchain in the healthcare sector.

# References


[1] Chika C Agbo and Qusay Mahmoud. Blockchain in healthcare: Opportunities, challenges, and possible solutions. *International Journal of Healthcare Information Systems and Informatics*, 15(3):82–97, 2020. doi: 10.4018/IJHISI.2020070105.

[2] Saud Alshehri, Stanisław P. Radziszowski, and Raj Kumar Raj. Secure access for healthcare data in the cloud using ciphertext-policy attribute-based encryption. In *2012 IEEE 28th International Conference on Data Engineering Workshops*, pages 143–146, 2012. doi: 10.1109/ICDEW.2012.68.

[3] José Luis Fernández-Alemán, Isabel Cristina Señor, Pablo A. Lozoya, and Ambrosio Toval. Security and privacy in electronic health records: a systematic literature review. *Journal of Biomedical Informatics*, 46(3):541–562, 2013.

[4] Alia Shahnaz, Usman Qamar, and Asma Khalid. Using blockchain for electronic health records. *IEEE Access*, 7:147782–147795, 2019. doi: 10.1109/ACCESS.2019.2946373.

[5] Pradeep Kumar Singh, Farjana Khanam Nishi, Mahizebin Shams-E-Mofiz, Mohammad Monirujjaman Khan, Abdulmajeed Alsufyani, Sami Bourouis, Punit Gupta, and Dinesh Kumar Saini. Electronic healthcare data record security using blockchain and smart contract. *Journal of Sensors*, 2022:7299185, 2022.

[6] Ye Xu, Yun Chi, and Zhuo Wang. Dynamic robustness and efficiency on link-weighted scale-free networks by gray infos. *Future Generation Computer Systems*, 107:865–870, 2020. ISSN 0167-739X. doi: 10.1016/j.future.2018.06.001.

[7] Buket Yüksel, Alptekin Küpçü, and Öznur Özkasap. Research issues for privacy and security of electronic health services. *Future Generation Computer Systems*, 68:1–13, 2017. ISSN 0167-739X.

[7], [2], [4], [5], [3], [1], [6].